作業四：AES

學號：C24106082
姓名：陳宏彰

2022-10-04

1 結果

密鑰：Hj%N)6tgZ}9wrc*m
明文：National Cheng Kung University
隱藏的四個字元是%、6、}、*

2 完整程式碼

https://github.com/simbafs/NCKU-IS-HW4

3 過程

3.1 解密函數

首先要先寫出可以解出範例密文的解密函數，原本想透過 openssl 解密，但參數一直調不對。最後用 go 的標準函式庫 ‘crypto/aes‘ 解密。解密函數在 aesUtil.go:54

3.2 暴力搜尋

有了解密函數，接下來就只須要在暴力搜尋中用不同金鑰去嘗試，如果符合條件就印出來，程式碼在 main.go:28

3.3 限制條件

如果把所有解密出來的字串都印出來，數量會大到無法處理，因此需要加上限制條件。首先是公告的 **明文字首**，透過這個條件篩選，大概剩下 3000 個符合字串。接下來根據助教回信，明文都是有意義的字串，因此我們可以加上限制每個字元都必須是「**可印的**」，雖然不是精準的「有意義的」，但已經篩選到 52 個字串。最後根據兩個條件的篩選，可以看到有意義的字串只有「National Cheng Kung University」，因此這個應該就是原本的明文了。

解密出來的結果在 plaintext:12、密鑰在 key:12